Freedom House

FREEDOM ON THE NET 2019

Thailand

NOT FREE

35 /100

A. Obstacles to Access	16 /25
B. Limits on Content	11 /35
C. Violations of User Rights	8 /40

LAST YEAR'S SCORE & STATUS

35 /100 Not Free

Scores are based on a scale of 0 (least free) to 100 (most free). See the research methodology and report acknowledgements.

Overview

The internet is severely restricted in Thailand. Ahead of the general elections in March 2019, the first to be held since the 2014 coup d'etat, the ruling junta moved aggressively to squelch support for the opposition and imposed an onerous regime of restrictions on social media. Opposition candidates were charged under repressive laws, while vague guidelines provided more power for content removal and restricted the use of social media for digital campaigning. A troubling new trend of enforced disappearances and mysterious deaths of prodemocracy and antimonarchy activists also emerged. Furthering this clampdown on online freedom, a draconian cybersecurity law went into effect at the end of the coverage period.

A military junta conducted a coup in Thailand in 2014, claiming that it would put an end to a political crisis that had gripped the country for almost a decade. As the military government imposed its rule, it exercised unchecked powers granted by the constitution to restrict civil and political rights, and to suppress dissent. The government that took power after the 2019 elections is led by Prime Minister Prayut Chan-ocha, the army chief who staged the 2014 coup and had declared himself prime minister in the immediate aftermath.

Key Developments, June 1, 2018 – May 31, 2019

- Manipulated, false, or misleading online content proliferated during the 2019 election campaign. Such content was mainly aimed at discrediting antimilitary parties and leaders including Thanathorn Juangroongruangkit, the leader of the more progressive Future Forward Party (see B5).
- Vague and restrictive rules imposed by the Election Commission of Thailand during the general election campaign limited the use of digital tools for political campaigning (see B2 and B8).

- A human rights lawyer was sentenced to 16 months in prison under the repressive Computer Crime Act (CCA) for commenting on the country's 1932 revolution. Candidates of the progressive Future Forward Party were also charged under the CCA for critical Facebook posts (see C3).
- In May 2019, a new cybersecurity law was enacted. It grants the government broad powers to access personal data and communications without judicial review (see C5).
- Three prodemocracy and antimonarchy activists living outside of Thailand were disappeared in December 2018. The mutilated bodies of two of them were found in January 2019, in the Mekong River on the border between Thailand and Laos (see C7).
- In May 2019, three antimonarchy activists who faced lèse-majesté charges were disappeared in Vietnam after leaving Laos. Civil society groups claimed that they were handed over to Thai authorities, an allegation they denied. The activists' whereabouts were unknown as of July 2019 (see C7).

A. Obstacles to Access

Internet access is considered affordable. While access has been steadily increasing, there remains a significant urban-rural divide. The government has worked to install free Wi-Fi access points in underserved areas, but their reach remains limited. Authorities have continued efforts to tighten technical control over infrastructure, as well as over telecommunications regulators. A handful of large providers dominate the telecommunications and internet-services market, and are all either government-controlled or thought to have close links with the authorities.

A1 0-6 pts	
Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?	**5**/6

Internet access is improving in Thailand, particularly as increasing numbers of users go online via their mobile phones. According to the International Telecommunications Union (ITU), 57 percent of people in Thailand accessed the

internet in 2018. *The Inclusive Internet Index 2019*, a project of the *Economist,* ranks Thailand 33 out of 100 countries in terms of availability, determined by quality and breadth of available infrastructure. [1]

Mobile internet penetration continues to steadily increase. By the end of March 2018, 94.7 percent of internet users accessed the internet using their mobile phone, compared to 93.7 percent in 2017. In contrast, 39 percent of users in 2018, down from 45 percent the previous year, accessed the internet through desktop computers, according to official statistics. [2]

Thailand's international bandwidth usage amounted to 6,627 Gbps in May 2018, and domestic bandwidth amounted to 5,869 Gbps, [3] about 62 percent and 37 percent higher than the same month in 2017, respectively.

In January 2019, the National Broadcasting and Telecommunication Committee (NBTC) announced that it expected to close 2G cellular networks by November 2019, in preparation for 5G to be rolled out in 2020. [4]

A2 0-3 pts	
Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?	**2**/3

There remains an inequality in internet access, largely based in socioeconomic class and geographical location.

However, the cost of access has continued to decrease. About 56 percent of internet users spend between 200 and 599 baht ($6 to 18) per month to access the internet, while 21 percent pay under 200 baht per month. Nearly 11 percent of the population access the internet through free programs. [5]

Government programs have sought to reduce the persistent digital divide between urban and rural areas. [6] Initiated in early 2016 by the then Ministry of Information and Communication Technology (MICT) and the National Broadcasting and Telecommunication Committee (NBTC), the "Return Happiness to the Thai People"

program aimed to provide broadband internet via wireless and fixed-line access points in rural areas at reasonable costs. As of January 2019, the National Council for Peace and Order (NCPO)— the military junta that seized power in 2014—had installed WiFi hotspots in 24,700 villages, although connectivity problems persist due to poorly managed maintenance systems. [7] The program also includes recruiting and training of people to work with villagers to develop ICT skills. [8]

A3 0-6 pts	
Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?	**5**/6

There were no reports of the state blocking or throttling internet or mobile connections during the coverage period of this report, although the government does have some technical control over the internet infrastructure.

The Communication Authority of Thailand (CAT) Telecom a state telecommunications provider, operates international telecommunications infrastructure, including international gateways, and connections to submarine cable networks and satellites. [9] Access to the international internet gateway was previously limited to CAT until it opened to competitors in 2006. [10]

Authorities continued on with a plan to merge CAT Telecom and TOT Telecom, both of which are state-owned. The merger received regulatory approval in May 2019, and the new entity, National Telecom, was set to begin operations in 2020. [11] While carried out in order to compete with private telecom companies, [12] these moves are also seen as part of the government's plan to consolidate its control over the country's telecommunication infrastructure.

Since 2006, the military has prioritized a "national internet gateway," aimed at allowing Thai authorities to interrupt internet access and flow of information anytime. [13] With the Thai military government no longer retaining full power following the March 2019 elections, it is unclear if this controversial "single gateway" will be implemented. [14]

A4 0-6 pts	
Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?	**4** / 6

High-speed internet packages are concentrated among a handful of large providers. Though many are privately owned, a United Kingdom–based Privacy International research report published in 2017 found that authorities for years have held "close relationships with private telecommunication companies and ISPs [internet service providers] through appointments which starkly exemplify the revolving door between the government and the private telecommunications sector." [15]

Although 20 ISPs have licenses to operate in Thailand, the three biggest operators in 2018 controlled almost 88 percent of the market. TRUE Online held the highest market share, with 37.8 percent toward the end of 2018. Jasmin followed with 32.4 percent, and state-owned TOT retained third place despite seeing its market share fall to 17.5 percent. [16] Advanced Info Service (AIS), Thailand's top mobile service provider, which entered the fixed-line broadband market in 2015, accounted for 7.4 percent. The company is expanding its fiber-optic network and growing at a rapid pace. [17]

For the mobile market, AIS saw a decrease of about 1 percent in its market share, which was at about 46 percent toward the end of 2018. Norwegian-controlled DTAC followed with 30 percent, and TRUE held 21 percent. [18] AIS and DTAC operate some spectrum under concessions from state-owned TOT and CAT Telecom—an allocation system that does not entirely enable free-market competition.

A5 0-4 pts	
Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?	**0** / 4

Following the 2014 coup, the military junta implemented reforms to the regulatory bodies overseeing service providers and digital technology that reduced their

independence, transparency, and accountability.

The NBTC, the former regulator of radio, television, and telecommunications, was stripped of its authority, revenue, and independence when the National Legislative Assembly (NLA) passed the NBTC Act in June 2017. It endures as a government agency half its original size, authorized to implement policy set by a commission led by the prime minister and other new entities with overlapping functions.

The Ministry of Digital Economy (MDES), one of the country's regulatory bodies, was established in June 2016 by the NLA. MDES replaced the Ministry of Information and Communication Technology (MICT) and is responsible for implementing policy and enforcing the Computer Crime Act (CCA) (see C2). [19]

The Commission for Digital Economy and Society (CDES), another official body, provides directives to MDES and is responsible for formulating policy under the 2017 Digital Development for Economy and Society Act (DDA). [20] Chaired by the prime minister, the commission is comprised of government ministers and no more than eight qualified experts. [21] It is stipulated as a legal entity, not a government body, absolving it of accountability under laws that govern government agencies, though it has authority over the MDES and the NBTC. The commission operates through the Office of the National Digital Economy and Society Commission. Section 25 of the Act mandates that the NBTC transfer revenue to that office "as appropriate."

The DDA redirects up to 5 billion baht ($165 million) of NBTC licensing revenue toward a new Fund for Developing Digital for Economy and Society, a broad legal entity authorized to regulate policy and receive profits from business joint ventures or its own operations. The act also effectively replaced a public body, the Software Industry Promotion Agency, with a similarly broad entity, the Office of Digital Economy Promotion (ODEP). Like the CDES, neither the Fund nor the ODEP is classified as a government body accountable to the public, leading to serious concerns about transparency and conflicts of interest.

The NBTC's nomination committee is comprised of seven people holding various bureaucratic and judicial positions affiliated with the government. Candidates are vetted by the senate secretariat and endorsed by the Senate. Candidates are no

longer required to have specific expertise in telecommunications, broadcasting, or other relevant fields per a January 2019 decision by the junta, though in effect they were already selected based on their rank in the government, military, or police, rather than relevant professional experience. NBTC commissioners are paid extremely well, and have significant influence over the multibillion-baht telecom businesses. [22]

In April 2018, the NLA rejected all 14 candidates that the NBTC nomination committee proposed. [23] Following the vote, the head of the NCPO suspended the nomination process under Section 44 of the interim constitution which is not subject to appeal, mandating that the previous commissioners continue in their roles. As of July 2019, the selection of commissioners was still pending.

B. Limits on Content

The government continues to restrict critical content online by blocking webpages and virtual private networks (VPNs), and by requesting that major companies like Google and Facebook remove content from their platforms on grounds that it violates the country's various restrictive laws. Disinformation proliferated online in the lead-up to and during the general elections in March 2019, while authorities imposed vague guidelines that limited political campaigning.

B1 0-6 pts	
Does the state block or filter, or compel service providers to block or filter, internet content?	**3**/6

Blocking of antiroyal content is widespread, but a lack of transparency means the extent of this blocking is unclear. Websites have been blocked on grounds of national security, antiroyal content, gambling, intellectual property, and hosting VPN services. [24]

In December 2018, the police's Technological Crime Suppression Division reported that it had requested that the Ministry of Digital Economy block more than 1,500 websites in 2018, most relating to gambling and intellectual property violations. [25] In

December 2018, the NBTC Secretary General revealed that it was not successful in blocking certain URLs because they were encrypted under the HTTPS protocol. The NBTC Secretary General reported that it would seek assistance from officials from both the United States and Japan, where the websites originate, to help block the URLs. [26]

Thailand has never publicly revealed the number of URLs blocked by court orders. Often, the public learns that a URL is blocked when they are denied access to that website. In May 2017, the Thai Internet Service Providers Association (TISPA) said its members blocked access to over 6,300 URLs pursuant to NBTC orders for threatening national security, a category that can include lèse-majesté content, hosting pornography, and facilitating gambling, among other issues. [27]

Some blocks affect entire websites, not just URLs for individual articles or posts. Researchers tested 1,525 URLs on six ISPs between November 2016 and February 2017, and found 13 websites completely blocked. [28] At least one news website, the United Kingdom's *Daily Mail,* was blocked at the domain level by TOT and 3BB. Websites offering tools for anonymity and circumventing censorship, as well as VPNs, are also blocked on more than one network. [29] The study revealed significant inconsistencies across ISPs, suggesting some providers may implement discretionary restrictions without prior authorization. The website of the VPN Hotspot Shield [30], for example, was blocked by the ISP True but otherwise available, while Ultrasurf, another VPN, was blocked by DTAC, AIS, and 3BB as of March 2019.

B2 0-4 pts	
Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content?	**0** / 4

Like blocking and filtering, content removal continued under the tight control of the junta government during the coverage period.

Ahead of the March 2019 general elections, the Election Commission of Thailand (ECT) set up a special unit to monitor for online posts that they deemed to be spreading misinformation and inflammatory content. When such content was found,

the ECT would notify those involved to remove the content, or request to platforms to do so. Under Section 73 (5) of the Organic Law on Election and the ECT's Regulation on Election Campaign respectively, authors of such content could also be punished with jail terms of up to 10 years, and banned from politics for 20 years. [31] Content the ECT ordered removal of, most of which was deemed to be false information about parties and candidates, targeted both anti- and promilitary parties. [32]

Between July and December 2018, Facebook restricted access to 584 items after receiving court orders or requests from the junta, on grounds that the content was lèse-*majesté*. This was double the amount of content removed the previous six months. [33] According to Google's transparency report, the government sent 150 requests to Google from January to June 2018 to remove 6,414 items. [34] Ninety-seven percent, or a total of 146 requests, were for criticizing the government, while two requests were related to defamation. One request was for "adult content" and an additional one was due to a religious offense. Google compiled with 93 percent of requests.

Users, publishers, and content hosts are pressured and intimidated to remove content. In June 2019, after the coverage period, a French satirist living in Bangkok was pressured to remove a music video mocking the NCPO's anthem from his social media accounts. Police officers visited his house and ordered him to sign a memorandum that such content was "improper" and damaged Thailand and its people. [35] During the same month, a comedian and group of high school students were also pressured by authorities to remove or apologize for social media content criticizing or joking about the junta.

Content providers or intermediaries have complied with removal requests in the past because they were subject to possible prosecution (see B3).

B3 0-4 pts	
Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?	**0** / 4

Restrictions on online content lack transparency and those penalized do not have access to an independent appeals process. While authorities do ask courts to block content, the judiciary in practice grants requests without scrutiny. [36]

Amendments to the CCA that took effect in May 2017 could empower more bodies to assess blocking requests and could expand the kind of content subject to blocking. Section 20 of the CCA authorized MDES officials to request court orders to block content that is deemed a threat to national security or contravenes public morals or public order. The 2017 amendments established a nine-member, ministry-appointed "computer information screening committee" which may also authorize officials to apply for court orders to block content. Three of its members must be from the media, human rights, and information technology sectors. Section 20(3) appears to authorize the committee to order restrictions on content that threatens public order or morals even if the content does not actually violate any law, meaning courts could be asked to issue orders to block legal content at the discretion of a committee that is not accountable to the public. [37] As of July 2019, the selection of committee members was still pending. [38]

In July 2017, a decree expanding on the amended Section 20 was enacted. The decree states that service providers must abide by court orders to block access to websites using technical measures. [39] The final draft of the decree was an improvement from an earlier draft, which said ISPs are required to take a proactive role in censorship and use "whichever means necessary" to block content.

Under the 2007 CCA, providers or intermediaries are subject to prosecution for allowing the dissemination of content considered harmful to national security or public order. [40] The amendments to the CCA provide some protection for intermediaries through a notice-and-takedown system. They also require rules and procedures for takedown requests and clearly grant immunity to "mere conduits" and cache operators.

Despite these positive developments, the amendments still contain considerable scope for abuse. The amended CCA appears to hold individuals responsible for erasing banned content on personal devices, though how it might be enforced

remains unclear. Section 16(2) states that any person knowingly in possession of data that a court has found to be illegal and ordered to be destroyed could be subject to criminal penalties. [41] Analysts feared the language could lead to the destruction of archival data, but there was no clear case of the provision being enforced since the law became effective in 2017.

In July 2017, a new MDES decree further modified intermediary liability. [42] The decree established a complaints system for users to report banned content and also incentivized intermediaries to act on every complaint to avoid liability. After receiving notice, intermediaries must remove flagged content within seven days for alleged false or distorted information, within three days for alleged pornographic content, and within 24 hours for an alleged national security threat. There are no procedures for intermediaries to independently assess complaints. There is also an onerous burden on content owners: to contest removal, owners must first file a complaint with police and then submit that complaint to the intermediary, who has final authority over the decision. Both companies and content owners who do not comply face imprisonment of up to five years.

The decree's 24 hour window requirement to remove national security-related content disregards a 2013 court ruling that 11 days is an acceptable amount of time for removing content relating to national security. [43] Additionally, the decree requires that intermediaries determine the legality of content, which could cause intermediaries to ultimately remove any content they think could result in a lawsuit—prioritizing protecting themselves over the public's right to know.

Some feedback from intermediaries regarding the MDES decree has been cautiously optimistic, particularly relating to the clear set of procedures and the relief of some burden to proactively monitor and remove content. However, there have been no cases on the decree's implementation as of yet.

B4 0-4 pts	
Do online journalists, commentators, and ordinary users practice self-censorship?	**1** / 4

Thailand's restrictive political environment encourages self-censorship online. Legal sanctions for online activity such as criticizing the government on Facebook are prevalent (see C3). The junta government has also made it known that it monitors social media to control political expression. [44]

Most Thai internet users self-censor on public platforms when discussing the monarchy because of the country's severe lèse-majesté law (see C2). In February, for example, news circulated that the antimilitary Thai Raksa Chart Party would nominate Princess Ubol Ratana, the older sister of King Vajiralongkorn, to become prime minister. Users only discussed the development in private online conversations, such as in secret Facebook and LINE groups, and not on public platforms, and Thai news outlets and journalists also refrained from reporting on it. Local outlets only began reporting on the news after her candidacy was officially announced, in fear of committing lèse-majesté. [45]

B5 0-4 pts	
Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?	**1** / 4

Manipulated false or misleading online content proliferated around the 2019 election campaign. Most such content aimed to discredit antimilitary parties and leaders like Thanathorn Juangroongruangkit, the leader of the more progressive Future Forward Party (FFP) and a candidate to become prime minister. Further, a report from the Oxford Internet Institute released in September 2019 identified Thailand as having coordinated cybertroop teams whose full-time staff members are employed to manipulate the information space on behalf of the government or political parties. [46] The report found evidence that such teams have undergone formal training and work to support preferred messaging, attack their opposition, and suppress critical content.

Thailand is alleged to have fake accounts run by both bots and human accounts, which most often manipulate content on Facebook and Twitter. Some of the

websites, Facebook pages, and news outlets putting out false content and doctored files around the 2019 election linked back to the News Network Corporation (NNC), [47] whose previous chairman was a member of the junta's NCPO. For example, a few days before the vote, a dubious audio recording was circulated on social media that was purported to be Thanathorn conspiring with the self-imposed exile and former prime minister, Thaksin Shinawatra. Internet users proved the clip was doctored after it was aired by Nation TV Channel, a promilitary outlet under NNC. [48]

Separately, an outlet called Thai Truth, which published a series of articles supporting the military in the lead-up to the election, was shown to be most likely operated by a member of the junta itself. [49] Internet users found that its privacy policy had nearly identical wording to that of a junta leader's website; [50] the website's domain name was also registered only a day before the junta website. [51]

In July 2019, after the coverage period, Digital Economy and Society Minister Puttipong Punnakanta announced an initiative to establish a Fake News Center, whose mission would be to combat false and misleading information on social media that jeopardizes people's safety or violates the CCA (see C2 and C3). [52] Some observers, including leaders of the Future Forward Party, note that the junta has not done anything to combat disinformation targeting opposition parties, and have expressed concerns that the center will be used to suppress critical and opposition voices. [53]

B6 0-3 pts	
Are there economic or regulatory constraints that negatively affect users' ability to publish content online?	**2**/3

Many outlets struggle to earn enough in advertising revenue to remain sustainable, limiting their ability to publish diverse content. A draft bill circulated during the coverage period could allow the imposition of large fines for ethics violations, further limiting outlets' resources; the bill also contains language that would incentivize a wide variety of outlets to register with authorities.

The draft Bill on the Promotion of Media Ethics and Professional Standards, originally proposed as the Media Reform Law, would limit both press freedom and online speech. The draft circulated in 2018 [54] would create a national professional media council that would issue codes of conduct to journalists and media outlets. The council would also rule on complaints and could impose a fine of up to 50,000 baht ($1,650) on a legal media entity, including either an outlet or group of journalists. In a positive development, the current draft removed originally proposed registration requirements, although it does incentivize registration by exempting media organizations from fines if they are registered. The bill includes a vague definition of media that can be interpreted to include social media pages and anyone routinely publishing to a wide audience. [55]

The NBTC has signaled its intent to target the amount of advertising revenue digital technologies receive in comparison to traditional broadcasters. In September 2018, the NBTC announced new efforts to tax over-the-top (OTT) content, or online video and other media not accessed through a subscription service, in order to create a level playing field for OTT and traditional broadcasters. [56]

B7 0-4 pts	
Does the online information landscape lack diversity?	**1** / 4

Social networks and digital media provide opportunities for sharing information that would typically be restricted in traditional media. However, the diversity of viewpoints available online has been limited severely by the enforcement of restrictive laws, including ones aimed at controlling online content, as well as content removals, economic restrictions, and self-censorship (see B2, B4, B6, and C3).

Nevertheless, Thailand has a vibrant social media space. According to the Global Digital Report 2019, a project of social media management platform Hootsuite and global agency WeAreSocial, there were around 51 million social media users by the end of 2018. The most popular platform in 2018 was Facebook, followed by YouTube, LINE, and Instagram. [57]

B8 0-6 pts	
Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?	**3**/6

Social media, chat applications, and online petition sites such as Change.org are available and are essential tools for digital activism under the junta government. For example, in early 2019, over 70,000 people signed a petition calling for the Thai government to not repatriate Hakeem Al-Araibi, a Bahraini soccer player and political refugee with residency in Australia, to Bahrain at the Bahraini government's request. [58]

However, vague and restrictive rules imposed by ECT during the general election campaign from January to March limited the use of digital tools for political campaigning. [59] The rules mandated that parties notify the ECT of what content they would publish and when. They also restricted the type of content that can be posted on social media to only candidates' names, candidates' photos, party affiliations, party logos, policy platforms, slogans, and candidates' biographical information. Parties and candidates could not "like" or share content about other candidates that was deemed defamatory or false. If candidates failed to comply with the guidelines, they could face up to a six months jail term, a fine of up to 10,000 baht ($330), or both. [60]

Due to apparent concerns about the vague, harsh nature of the rules, some candidates, such as the Pheu Thai Party's prime minister candidate, Sudarat Keyuraphan, resorted to deactivating their Facebook pages. [61]

C. Violations of User Rights

In a disturbing development, some prodemocracy and antimonarchy activists disappeared from neighboring countries or were found dead. Internet users, including opposition candidates, continued to be charged and imprisoned for their online activity during the reporting period. Meanwhile, a draconian cybersecurity law that provides sweeping power to authorities went into effect in May.

C1 0-6 pts	
Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?	**1** / 6

The constitution drafted by the military government went into effect in April 2017, months after it was approved in a tightly controlled national referendum. It replaced an interim constitution introduced after the coup d'etat in 2014. However, Article 44 of the interim constitution, which gives the NCPO unchecked powers to issue any legislative, executive, or judicial order without accountability, was still in effect for the entire duration of this reporting cycle. [62] In July 2019, beyond the reporting period, Section 44 became obsolete when the newly elected government, still led by Prime Minister Gen Prayut Chan-ocha, was royally appointed. [63]

The 2017 constitution enshrined basic rights, but Section 25 stipulates that all rights and freedoms are guaranteed "insofar as they are not prohibited elsewhere in the constitution or other laws;" and that the exercise of those rights must not threaten national security, public order, public morals, or any other person's rights and freedoms.

The NCPO-appointed government during its four-and-a half-year term passed a number of laws to consolidate its power. Many have reduced the efficiency and transparency of independent regulators and government agencies in the name of "reforming" bureaucracy and the media.

Constitutionally, Thailand's judiciary is independent, but in practice courts are politicized and corruption is common. However, some courts have dismissed problematic online defamation cases under the CCA's Article 14, some of which dealt targeted government criticism on social media (see C3).

C2 0-4 pts	
Are there laws that assign criminal penalties or civil liability for online activities?	**0** / 4

A number of laws impose troubling criminal and civil penalties for online activities, and police and the attorney general's office continued to pursue criminal charges that clearly infringe on basic rights during the coverage period.

A revised CCA was adopted in December 2016. Among other things, it revised a section 14(1) of the original 2007 law that banned introducing false information into a computer system, which experts understand to refer to technical crimes such as hacking. [64] Judges, however, had shown limited understanding of this application, and the clause was widely used in conjunction with libel charges to prosecute speech. Observers say this provided grounds for Strategic Lawsuits against Public Participation (SLAPPs), allowing government officials and large corporations to file charges in order to intimidate and silence their critics. Lawmakers sought to limit this abuse by adding new language that excluded the measure's application in conjunction with defamation offenses. [65] Yet the law retained the problematic term "false" computer information, and added another, "distorted" computer information. As a result, the incorrect interpretation of the law persists and individuals continue to face charges for publishing allegedly false content on the internet (see C3).

Other problematic sections of the CCA also went unchanged, including Section 14(3), which criminalizes online content deemed to "affect national security" and is frequently used in conjunction with lèse-majesté charges. The revised CCA also extended the scope of online censorship and altered the legal framework for intermediary liability (see B3).

The country's criminal code also targets legitimate online activities (see C3). Sedition is covered under Article 116, for example.

Legislation that was pending during the coverage period includes the Bill on the Promotion of Media Ethics and Professional Standards, which could limit both press freedom and online speech with fines of up to 50,000 baht ($16,500) for any outlet deemed to break media ethics (see B6). The draft went to a public hearing in early 2019.

Under a separate draft law for the prevention and suppression of materials that incite "dangerous behavior," creating and distributing information deemed to provoke

behavior such as certain sexual acts, child molestation, or terrorism would be punishable by one to seven years in prison with fines up to 700,000 baht ($23,100). [66] The draft was still pending at the end of reporting period.

C3 0-6 pts	
Are individuals penalized for online activities?	**1** / 6

Despite the junta's talk of reconciliation and reform, criminal prosecutions against opposition figures for online activities remain common, and authorities continued exploiting Article 14 of the CCA to silence activists and opposition politicians during the coverage period. There were no new long-term convictions for online activities, save one resulting in a 16-month prison sentence.

Ordinary voters and party candidates alike were charged under the CCA during the 2019 election period. In March, nine internet users were charged for sharing "false" information about the ECT, amid criticism of the commission's outsized role in the general election. [67] Three newly elected members of congress from the anti-junta FFP—Thanathorn Juangroongruangkit, Klaikong Waithayakan, and Jaruwan Saranket—were charged in February 2019 under the CCA after criticizing the junta in a Facebook live broadcast. As of July 2019, the prosecutor had yet to bring official charges. [68] Pongsakorn Rodchompoo, another newly elected FFP lawmaker, was charged for sharing a doctored photo aimed at discrediting junta leader General Prawit Wongsuwan. Although Pongsakorn said he deleted the photo three minutes after posting when he realized it was fake, the police accused him of violating the CCA. [69]

In addition to election-related cases, users were charged, and in some cases convicted, under a range of laws, including the CCA and the criminal code. Many of the cases were politically motivated and intended to target activists. In February 2019, police charged Runapob Shinawatra, deputy leader of Thai Raksa Chart Party, for importing false information on Facebook. Amid pollution crisis in Bangkok in early 2019, Runapob launched an application where users could request dust levels based on their location. The police alleged the app did not accurately assess location data

and reported the incorrect level of dust. [70] In February 2019, a criminal court accepted a case against 10 internet users under Article 14 of the CCA. The 10 were accused of sharing a Facebook post defaming NCPO leader and Prime Minister General Prayut Chan-ocha and General Prawit Wongsuwan. [71] As of July 2019, the case is ongoing.

In February 2019, 11 people were arrested for spreading rumors that the military government will extend the conscripted period from two years to four years. Two of them were accused of posting the rumors themselves onto jookthai.com, while nine others were accused of sharing the news on the internet. [72] In December 2018, five people were convicted under the CCA for sharing rumors about the military government and policies on illegal drugs on Facebook. Each defendant, having pled guilty, was sentenced to six months in prison with 2,500 baht ($820) fine, with the prison term reduced to two year suspensions. [73]

In October 2018, Thammasaket Company, a poultry company based in central Thailand, filed a criminal and civil defamation lawsuit against Sutharee Wannasiri, then-Thailand human rights specialist for Fortify Rights, for her tweets which commenting on a short video related to another lawsuit brought by the company against its former 14 migrant works from Myanmar. [74] As of July 2019, both civil and criminal cases against Sutharee were pending trial before the courts. [75]

In September 2018, 12 people were arrested under the CCA for sharing content on Facebook claiming that police ignored an alleged rape of a British woman on the tourist island Koh Tao. Arrest warrants were also issued for a British editor of an online outlet and CSI LA, a Facebook page administrator based in the United States, both of whose outlets had accused the police of covering up a rape case. [76]

And in June 2018, human rights lawyer Prawet Praphanukul was convicted of three sedition charges under Article 116 of the Criminal Code and sentenced to 16 months in prison. [77] Prawet was arrested in 2017 for Facebook posts on the country's 1932 revolution. Prawet was originally also charged with lèse-majesté, but these were later dropped.

There were three positive developments in existing cases during the coverage period. First, in February 2019, an appeals court affirmed a lower court's decision in finding activist Rinda Pornsiripitak not guilty of violating the CCA for posting to Facebook a rumor about the unusual wealth of Prime Minister Prayut Chan-ocha that was allegedly false and could lead to public panic. The court ruled that Rinda was not influential enough to cause public panic, which is necessary under the CCA. [78] Also in February 2019, a court dismissed the computer crime and criminal defamation charges against patient's rights activist Preeyanan Lorsermvattana, who had critiqued Thailand's Medical Council on Facebook. [79] And in December 2018, a court found Pheu Thai Party politician Watana Muangsook not guilty of violating the CCA for his online comments related to the disappearance of a historical plaque. The court reasoned that Watana's speech related to academic freedom and not a computer crime. [80]

C4 0-4 pts	
Does the government place restrictions on anonymous communication or encryption?	**2** / 4

The government has attempted to restrict encryption, and has seen some success in limiting online anonymity.

In February 2018, the NBTC implemented a 2017 NRSA policy affecting the anonymous use of the internet. The new regulation requires mobile operators to collect fingerprints or face scans from SIM card registrants. The data must then be sent to a central repository at NBTC. [81]

In early 2017, the government took steps to undermine encryption. Section 18(7) of the amended CCA enables officials to order individuals to "decode any person's computer data" without a court order. [82] While some companies may be unable to comply with such orders, the law could provide grounds to punish providers or individuals who fail to decrypt content on request. Privacy International has reported on other possible ways for Thai authorities to circumvent encryption, including impersonating secure websites to intercept communications and passwords, and conducting downgrade attacks, which force a user's communications with an e-mail

client through a port that is unencrypted by default. [83] The group challenged Microsoft for trusting Thai national root certificates, leaving them vulnerable to measures that would undermine security for users visiting certain websites; Microsoft said a trustworthy third party vets authorities that issue certificates before the company accepts them. [84]

C5 0-6 pts	
Does state surveillance of internet activities infringe on users' right to privacy?	**1** / 6

The junta government actively monitors social media and private communications with limited, if any, oversight. A complex set of policies aim to control online communication, but the country lacks a legal framework establishing accountability and transparency mechanisms for government surveillance.

In May 2019, a new cybersecurity law, the Emergency Act of the Cyberspace, was enacted; it provides sweeping powers to the government to access personal data and communications without judicial review. [85] The law, which can be activated in response to "threats that affect or may affect the law and order," mandates three new committees to deal with three levels of threats—not serious, serious, and critical. Threats classified as "serious" and "critical" allow the government to bypass the judiciary when invoking the law, and permits actions including questioning and eavesdropping on people, searching property, collecting data and information in real time, accessing computer data and networks, and confiscating and copying electronic devices. All such actions may be carried out without a court order; [86] courts only need to be informed of searches and seizures retroactively.

In July 2017, the NRSA endorsed a set of policies that would systematize and increase the efficiency of government surveillance and its censorship apparatuses. [87] A National Reform Plan was to have established a central social media watch system and a new, centralized database for mobile phone users, both of which would have significantly increased the government's surveillance capabilities. [88] However, there were no reports during the reporting period suggesting that the systems had been established.

There have been prosecutions in previous years in which private chat records were used as evidence against internet users. It is not clear how officials accessed chat records in these cases, though military and police authorities have created fake accounts in order to join secret chat groups, even baiting users to criticize the monarchy or the junta. [89] In several cases in which individuals were summoned or arrested, the authorities also confiscated smartphones to access social media accounts.

A number of draft laws would enable more government surveillance. For example, a revised criminal procedural law still pending in mid-2019 would grant surveillance powers to authorized police officials. The draft stipulates a wide range of offenses for which surveillance is lawful; in addition to violations of national security and organized crime, it includes broad categories like "complex" crimes. [90] Under a separate draft law for the prevention and suppression of materials that incite "dangerous behavior," officials would require a warrant to access any private information that is deemed to provoke behavior such as certain sexual acts, child molestation, or terrorism.

Government agencies also possess surveillance technologies. Some bought spyware from the Milan-based Hacking Team between 2012 and 2014, according to leaked documents; [91] Thailand has also obtained licenses to export telecommunications interception equipment from Switzerland and the United Kingdom. [92] According to Privacy International, the licenses indicate the probable acquisition of IMSI (International Mobile Subscriber Identity) catchers, devices which intercept data from all phones in the immediate area regardless of whether they are the focus of investigation.

C6 0-6 pts	
Are service providers and other technology companies required to aid the government in monitoring the communications of their users?	**1** / 6

Instead of clear procedures, surveillance is facilitated by "the Thai government's control of the internet infrastructure [and] a close relationship with internet service providers," according to Privacy International. [93] CCA amendments allow officials to

instruct service providers to retain computer traffic data for up to two years, up from one year as mandated in the 2007 version. Providers must otherwise retain data for at least 90 days under the law. Though official requests to access that data require a warrant, a 2012 cabinet directive placed several types of cases, including CCA violations, under the jurisdiction of the Department of Special Investigation (DSI). Under rules regulating DSI operations, investigators can intercept internet communications and collect personal data without a court order, so internet users suspected of speech-related crimes are particularly exposed. Even where court orders are still required, Thai judges typically approve requests without serious deliberation.

The MDES established a cybersecurity center based in state-owned telecommunications company TOT to monitor for inappropriate content (see B3). [94]

Facebook and Google reported a handful of government requests to access user data in 2018. Google received four requests for data regarding five users or accounts, but complied with none between January and June. [95] Facebook received two requests for data regarding two users or accounts and provided none between January and June 2018. Between July and December 2018, Facebook received three requests for data about seven user accounts and provided 33 percent of data requested. [96] LINE, the most popular chat application in Thailand, reported receiving no requests from law enforcement for user data in 2018. [97]

C7 0-5 pts	
Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities?	**0** / 5

This coverage period saw extralegal intimidation, enforced disappearances, and mysterious deaths of prodemocracy and antimonarchy activists, based both in and outside of Thailand, in apparent connection with their online and offline actions.

After the coup in May 2016, more than a dozen of Thai prodemocracy activists fled Thailand to continue their political engagement online, much of which criticized and

parodied the Thai monarchy and advocated for a republic. In May, three antimonarchy activists—Siam Theerawut, Chucheep Chivasut, and Kritsana Thaptha—who face lèse-majesté charges, were disappeared in Vietnam after leaving Laos. Civil society reported that they were handed to Thai authorities, a claim General Prawit Wongsuwan denied. [98] Their whereabouts remained unknown as of July 2019.

In December 2018, another three prodemocracy and antimonarchy activists—Surachai Sae Dan, Kraidej Luelert, and Chatchan Buphawan—who were living in Laos, disappeared. [99] In January 2019, the bodies of Kraidej and Chatchan were found on the shore of the Mekong River bordering Thailand and Laos. Surachai's whereabouts remain unknown. The United Nations and civil society organizations have expressed concern over these disturbing developments; [100] the government has denied any responsibility. [101]

In addition to enforced disappearances, prodemocracy activists who are vocal online were assaulted during the coverage period. Sirawit Seritiwat, for example, was assaulted twice in recent months, while Ekkachai Hongkangwan has been assaulted at least seven times since January 2018. [102] The Thai police have not conducted thorough investigations into the attacks and have not provided bodyguards to the activists.

C8 0-3 pts	
Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?	**2**/3

There were no notable politically motivated cyberattacks reported during the coverage period. Private sector actors, however, were subjected to technical attacks. Toyota Thailand reported an online security breach in March 2019, for example. [103]

A leading antimilitary online news outlet, Prachatai, [104] has been subject to distributed denial-of-service (DDoS) attacks, though no major attacks were documented during the coverage period of this report. Sites of prominent dissident

rights groups such as iLaw [105] and Thai Lawyers for Human Rights [106] also reported no attacks during the reporting cycle. [107]

Hackers targeted government sites in previous years, notably in protest when the NLA passed the CCA in December 2016. Websites operated by several government agencies were defaced by hackers who displayed a symbol that was developed to oppose a plan to strengthen control of the internet by imposing a single gateway; [108] others were brought offline by DDoS attacks. Several people suspected of involvement were subsequently arrested and interrogated at a military base, [109] including a 19-year-old. [110]

In January 2017, Privacy International reported that the authorities have the capability to use downgrade attacks or man-in-the-middle attacks to circumvent encryption.

• • •

Footnotes

1 "Availability rankings," The Inclusive Internet Index 2019, The Economist Intelligence Unit, https://theinclusiveinternet.eiu.com/explore/countries/TH/?category=ava....

2 National Statistical Office, The 2018 (1st Quarter) Household Survey on the Use of Information and Communication Technology, October 29, 2018, https://perma.cc/U88U-EQR9.

3 Internet Information Research Network Technology Lab, "Internet Bandwidth in Thailand and International," National Electronics and Computer Technology Center, http://webstats.nbtc.go.th/netnbtc/BANDWIDTH.php.

4 Komsan Tortermvasana,

5 National Statistical Office, The 2018 (1st Quarter) Household Survey on the Use of Information and Communication Technology, 2018, http://tinyurl.com/y2xn2x5y; The National Broadcasting and Telecommunications Commission (NBTC), Report on the ICT Market for the 3rd Quarter of 2018, 2018, nbtc.go.th/Business/commu/telecom/informatiton/research/**รายงานสภาพตลาดโทรคมนาคม/ปี**-2561/35738.aspx.

More footnotes ⊕

On Thailand

See all data, scores & information on this country or territory.

See More >

Country Facts

Global Freedom Score

36 /100 **Partly Free**

Internet Freedom Score

39 /100 **Not Free**

Freedom in the World Status

Not Free

Networks Restricted

No

Social Media Blocked

No

Websites Blocked

Yes

Pro-government Commentators

Yes

Users Arrested

Yes

In Other Reports

Freedom in the World 2019

Other Years

2023

Be the first to know what's happening.

Join the Freedom House weekly newsletter

Subscribe

ADDRESS

1850 M St. NW Floor 11
Washington, DC 20036
(202) 296-5101

GENERAL INQUIRIES

info@freedomhouse.org

PRESS & MEDIA

press@freedomhouse.org